

U.S. SEAPORT SECURITY: CRITICAL CHALLENGE FOR DEPARTMENT OF HOMELAND SECURITY

BY

COLONEL DREFUS LANE, SR.
United States Army

DISTRIBUTION STATEMENT A:

Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2009

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.



U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 02-04-2009		2. REPORT TYPE Strategy Research Project		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE U.S. Seaport Security: Critical Challenge for Department of Homeland Security				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Colonel Drefus Lane, Sr.				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Dr. Dallas Owens Strategic Studies Institute				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT <p>United States Seaports are vital to the US economy and national security. During the post 9/11 port assessments, the U.S. Maritime Transportation System (MTS) was cited as security vulnerability. The 9/11 terrorist attacks tragically demonstrated the vulnerability of the United States to asymmetric warfare.</p> <p>This Strategic Research Project (SRP) focuses on (1) security threats and vulnerabilities of U.S. Seaports; (2) the roles, responsibility, and strategies taken across the full spectrum of government to improve security of U.S. seaports; and (3) port security issues and challenges remaining.</p>					
15. SUBJECT TERMS Maritime Domain Awareness, Port Security Vulnerability					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UNLIMITED	18. NUMBER OF PAGES 26	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			19b. TELEPHONE NUMBER (include area code)

USAWC STRATEGY RESEARCH PROJECT

**U.S. SEAPORT SECURITY: CRITICAL CHALLENGE FOR DEPARTMENT OF
HOMELAND SECURITY**

by

Colonel Drefus Lane, Sr.
United States Army

Dr. Dallas Owens
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Drefus Lane, Sr.

TITLE: U.S. Seaport Security: Critical Challenge for Department of Homeland Security

FORMAT: Strategy Research Project

DATE: 02 April 2009 WORD COUNT: 5,122 PAGES: 26

KEY TERMS: Maritime Domain Awareness, Port Security Vulnerability

CLASSIFICATION: Unclassified

United States Seaports are vital to the US economy and national security. During the post 9/11 port assessments, the U.S. Maritime Transportation System (MTS) was cited as security vulnerability. The 9/11 terrorist attacks tragically demonstrated the vulnerability of the United States to asymmetric warfare.

This Strategic Research Project (SRP) focuses on (1) security threats and vulnerabilities of U.S. Seaports; (2) the roles, responsibility, and strategies taken across the full spectrum of government to improve security of U.S. seaports; and (3) port security issues and challenges remaining.

US SEAPORT SECURITY: CRITICAL CHALLENGE FOR DEPARTMENT OF HOMELAND SECURITY

Seaports are not a separate mode of the transportation system; rather seaports enable sealift capability to connect to other surface modes. There are an estimated 360 seaports in the U.S. These seaports annually handle roughly 1.5 billion tons of cargo worth over \$1 trillion, arriving in at least 11 million containers. These statistics are rapidly growing. These seaports require deep-water access, sufficient land for staging and storage, and unrestricted access to highway, rail, inland waterway, and pipeline networks.

Seaports are generally run as self-sufficient business enterprises; they have access to various forms of funding sources for improvements. Participating companies function in a wide variety of capacities- such as container/cargo terminal operators, port authority managers, stevedoring, and shipper's agents. The Department of Defense (DOD) maintains only an informal business relationship with U.S. ports. However, it plays a considerable role in the security plan to prevent attacks on the seaport, prepare to respond to possible attacks, and to restore their services.

The 9/11 terrorist attack on the World Trade Center in New York and on the Pentagon instantly created a new American consciousness of the homeland's vulnerability to terrorism. Political will rose to an unprecedented level to address the nation's new priority of protecting the homeland. In the aftermath of 9/11, the President then created the Department of Homeland Security to develop and implement a comprehensive national strategy for homeland security.

The 2004 Presidential Directive for Maritime Security Policy mandated that the collaboration between state, local, and private sector entities be conducted at the federal level to achieve complete and unified maritime security programs and initiatives.¹ Thus, U.S. seaports have been designated vital to the US economy and national security strategy. The maritime transportation system was identified as an easy target as a result of the 9/11 commissions investigations. Seaports were considered to be the most vulnerable sectors that could affect U.S. economy.² This SRP contributes to port security awareness of maritime programs by providing a preliminary assessment of U.S. seaports security.

It begins with an assessment of implicit security threats and vulnerabilities to US seaports before and after 9/11, including a review of policies and regulations affecting U.S. Seaports. It discusses major background issues relating to security challenges and vulnerabilities of the maritime transportation system (MTS) pertinent to US Seaports, including the roles and preparedness of Federal, state, and local agencies before and after the September 11 attacks. It concludes with a summary of remaining challenges and issues regarding U.S. seaport security.

Security Threats and Vulnerabilities

U.S. Seaport Security Threats and Vulnerabilities Prior to 9/11. U.S. Seaports are naturally at risk to terrorist attacks due to their huge land masses. It is common for seaports to have many avenues of access, by water and land. They are often located in metropolitan areas. They transport large quantities of valuable goods, and provide effective transportation links and nodes to many destinations within U.S. borders. The perceived pre- 9/11 threats and vulnerabilities included internal conspiracies,

stowaways and smuggling illegal aliens, illegal export, and drug smuggling. Defending against these vulnerabilities proved difficult due to the staggering numbers of U.S. ports and their structural designs.

The mission of defending our ports requires us to “uphold U.S. maritime sovereignty and enforce U.S. law, international conventions, and treaties against criminal activities.”³ “The Federal government has the [overall jurisdiction] over harbors and interstate and foreign commerce, but state and local governments are the main port regulators.”⁴ The United States Coast Guard (USCG) is empowered to enforce all laws, conventions, and treaties in the maritime domain, crafted to suppress illegal migration, human trafficking, smuggling drugs and other contraband, and all other federal or international crime. This enforcement plays an integral role to secure air, land, and sea borders.

U.S. Seaport Security Threats and Vulnerabilities after 9/11. US Seaports are vital assets to the US economy and national security strategy. “One of the most vulnerable sectors of the U.S. economy identified during [post 9/11] assessments was the maritime transportation system (MTS), specifically U.S. seaports’ [vulnerability].”⁵ The 9/11 attacks tragically demonstrated the vulnerability of the United States to attacks.⁶ The Al Qaeda network demonstrated to the world that terrorist attacks have the potential to disrupt the global economy.⁷

The U.S. federal government immediately started assessing its vulnerability to these threats across a wide-range of possibilities and designated numerous government and non-governmental facilities as critical infrastructure, to include U.S. seaports. This post-9/11 sense of uncertainty has permeated the national security environment.

Vulnerabilities Pose Security Risks. There are various physical and infrastructural dimensions amongst seaports throughout the United States however; several have similar designs which cause them to be at risk to terrorist attacks.⁸ These characteristics are relevant to both their framework and structure. These approaches make securing such expansive areas of entry even more complex when implementing security measures. Ports located in large industrial areas make it hard to execute the required security measures. Ports are largely located in urban areas where commercial activities involving fuel resources, storage and handling of hazardous products and materials are key components of the infrastructure. The dynamics of these arrangements are compounded because of the close location to bridges, railroads and industrial facilities. In addition, maintaining the ingress and egress of materials in these locations is of critical importance to the security and financial stability of the economies in this environment. Again facts such as these make the infrastructure, land and ports prime targets for illegal and terrorist activities.⁹

Initiatives to Strengthen Port Security

Governmental agencies have taken aggressive actions to mitigate risk associated with potential threats and vulnerabilities of the U.S. seaports since 9/11.¹⁰ The Department of Homeland Security (DHS) has been a key source for identifying and developing solutions to diminish some of the security challenges. DHS has taken the lead in implementing the directives established by Executive Order and both Houses of Congress.¹¹ The U.S. Coast Guard and two other key DHS agencies play a significant role: the U.S. Customs Service, which is sustaining an ongoing initiative for ensuring the security of cargo entering U.S. ports, and the U.S. Immigration and Naturalization

Service (INS), which is also addressing issues that include inspections of individuals, containers trying to enter the United States.¹² The Federal role extends beyond these three agencies. The Department of Justice (DOJ), Department of Agriculture (DOA), and, Department of Commerce (DOC), Department of Labor (DOL) and Department of State (DOS) collaborate regularly with the Federal Maritime Commission and other related agencies to develop strategies and implement policies to address these complex issues associated with materials handling storage, ingress and egress and the disposition vessels in and around US ports.¹³

Security measures along the U.S. coastlines exceeding thousands of miles of unoccupied territory presents a target of opportunity for illegal entrance into the United States. This vulnerability demands a more robust strategy from agencies patrolling the sector of land mass. Better surveillance, coordination and communications are required for a well defined strategy to maintain control over maritime borders and access points. These robust initiatives could help reassure U.S. citizens that the borders are safe and secure and dissuade terrorist threats and activities. In addition, this strategy will help improve mobile surveillance and increase early detection of potential events and activities that could threaten the security of facilities and measures to provide the capability to deter and if necessary “engage adversaries well before they can cause harm to the United States”.¹⁴

Legislations Governing the Defense of US Seaport Security

A number of studies conducted prior to 9/11 identified the serious vulnerability to terrorism facing the U.S. These efforts clearly informed our officials that the U.S. continues to be threatened by international terrorist organizations. Reports and

legislative bills identified Osama Bin Laden and the Al Qaeda network as serious threats. Subsequently, a plethora of national security recommendations indicate how the nation and the military should posture for potential attacks on U.S. seaports. They identify appropriate roles for the Department of Homeland Security and the Department of Defense. Congress then passed bills to support national security efforts to protect the homeland.

A bill to establish The Graham Commission was introduced on 20 July 2001, by Senators Hollings and Graham. This “bill is similar to legislation [S2965] introduced in the 106th Congress on [27 July 2000] in response to the findings of the Interagency Commission on Crime and Security in U.S. Seaports.¹⁵ Its provisions provided guidance to the Coast Commandant that directed the development of a Task Force to enact congressionally mandated provisions. The provisions also called for the establishment of port security committees to centralize and coordinate with port authorities and members of law enforcement at the local level. Some other provisions included: establishing local port security committees at each U.S. seaport; developing port security threat assessments at least every three years; and recommending ‘best business practices’ guidelines for use by maritime terminal operators.

The Hollings Bill was passed by the Senate in Nov 2002 to establish the Graham Commission. The Hollings Bill addresses a broad range of seaport crimes, but focus on terrorism, and its provisions include:¹⁶

- Created a National Maritime Security Advisory Committee
- Established local port security committee
- Mandated assessment of port security and vulnerability assessments

- Required security plans for port facilities
- Called for controlled access to port facilities
- Enhanced cargo documentation procedures
- Sought to control foreign port security procedures – sanctions
- Enhanced Coast Guard waterside security
- Established a Sea Marshal program
- Recognized participation of agencies outside of the Department of Transportation (DOT)

Terrorist Attacks Are Not New

Terrorism is not a new phenomenon. There is a long history of terrorist attacks against the United States at locations all over the world. Most of these were relatively insignificant attacks intended to call attention to particular local issues. Within the last decade, most attacks against the U.S. have occurred outside its borders. For example, more than 2,100 international terrorist attacks occurred between 1995 and 2000, with only 15 occurring in North America.¹⁷ As a result, prior to 9/11, terrorism was not an important issue for most Americans.

The methods used on 9/11, hijacking airplanes and using airplanes as missiles are not new. Over 500 hijackings have been recorded since the early sixties.¹⁸ During World War II (WWII) the Japanese used airplanes in suicidal attacks to target U.S. warships. More than 3,900 Japanese pilots executed these types of attacks by flying “kamikaze missions.”¹⁹ What is new is the combination of these suicidal tactics used within our borders.²⁰

After the Cold War, the world's economy became more global and the U.S. became the only remaining superpower following the fall of the Soviet Union. Terrorism assumed a greater dimension in the 1990s with its new goal of producing mass casualties with little regard for achieving specific political goals or for consistently claiming responsibility.²¹ Over the last decade terrorists have exhibited an increased willingness to inflict numerous casualties. It is now clear that terrorists intend to continue attacks against the U.S. and cause significant civilian casualties. To date there have been no known terrorist attacks on U.S. ports.

These type threats are unique and unpredictable and the 9/11 attacks sent a clear message that the United States, as the world's sole superpower and even while enjoying conventional and nuclear supremacy, is vulnerable to asymmetric attacks from non-state actors and militarily inferior opponents. Terrorist attacks involve the non-traditional use of strategies, tactics, and weapons by those seeking to circumvent the strength and attack the vulnerabilities of dominant opponents. Terrorist attacks on and against the U.S. have exhibited increasingly bold and violent efforts to avoid direct confrontation with U.S. military powers in favor of improvising means to exploit perceived weaknesses.

The broad range of potential terrorist attacks include the use of nuclear, chemical, and biological weapons and attacks on information operations, as well as uses of unconventional weapons such as commercial aircraft. Such threats are formidable because of their lethality; they can be delivered by a broad range of systems, from sophisticated ballistic or cruise missiles to simple fishing vessels, trucks, commercial airplanes, and devices made from household goods or industrial chemicals.

Terrorists have proven persistent and adaptive in employing technology and exploiting security weaknesses.

Weapons of Mass Destruction (WMD) attacks and threats require coordinated responses with participation among all levels of government and the Department of Defense. Military and civilian capabilities must be joined with a coordinated effort to thwart WMD attacks. DOD has unique assets in expertise, training, and equipment. The military can support civilian authorities with specialized response teams, joint task forces, and the National Guard Weapons of Mass Destruction Civil Support Teams (WMD CSTs). In a joint operation these teams play a role as part of an overall effort to provide responders with technical and medical assistance in the critical period immediately following a WMD event. Support for civil authorities' response to chemical, biological, radiological, nuclear, and electronic attacks (CBRNE) should be a primary military mission. This support involves both a direct CBRNE response and the National Guard and Army Reserve training and equipping of local first responders to chemical and biological attacks and other security missions.

Federal Agency Responsibilities for Homeland Security

Following 9/11, protecting the U.S. homeland from future attacks quickly became the nation's primary security concern, and Americans demanded immediate action. The creation of the Department of Homeland Security (DHS) by President George W. Bush, formalized new federal responsibilities for homeland security.²² DHS also assumed overall responsibility for U.S. seaport security. The new office mission and functions are.²³

- To develop and coordinate the implementation of a comprehensive national strategy to defend the homeland.

- To coordinate the federal efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the U.S.

To support the DHS initiative, Congress gave the President a 40 billion dollar supplemental allocation for port security. The nation's sense of urgency to protect the homeland, as well as to pursue and destroy any terrorist, became the new strategic aim. Less clear, however, was exactly who needed to do what to ensure protection of the homeland, at what cost, and at what tradeoffs in civil liberties.

Subsequently, various stakeholders in the nation's homeland security have developed a construct to implement a flexible program to strengthen deterrence against terrorist threats on U.S. seaports. It is not surprising that the level of emphasis being placed on port security since 9/11 attacks has increased immensely. Governmental agencies at all levels are collaborating to develop a consistent plan of action, but their levels of effort are not the same at all locations.²⁴

The USCG has long been responsible for protecting ports, harbors, vessels, and waterfront facilities from accidents, criminal acts, terrorism, and sabotage.²⁵ After the 9/11 terrorist attacks, the Coast Guard was granted new authority as the Federal Maritime Security Coordinator (FMSC) within U.S. ports and adjacent waters.²⁶

The USCG is not solely responsible for port security. Other agencies and organizations subordinate to DHS, with specialize port security missions, include the U.S. Customs and Border Protection (CBP) and the Directorate for Border and Transportation Security (BTS). The CBP is responsible for screening, inspection, and examining, international cargo and individuals attempting to enter U.S. through maritime ports.²⁷

The Coast Guard, the U.S. Customs Service, U.S. maritime stakeholders, and interagency partners along with the international community is actively updating and strengthening existing maritime initiatives and building new initiatives where needed to address emerging challenges and threats. GAO Report indicates that some of its important actions in port security include the following:²⁸

Conducting initial risk assessments of ports. Seaports throughout the nations are being assisted by the Coast Guard safety teams personnel, who are conducting facilities and critical infrastructure risk assessments to help determine where there are most vulnerable which allow them to immediately implementing corrective actions to reduce or eliminate the threats.

Redeployment Assets. Coast Guard assets were redistributed to several larger ports such as, San Francisco, Boston, New York, and Miami facilities throughout the United States in an effort to support border patrolling and local law enforcement on-going activities design to reduce illegal smuggling of drugs and aliens.

Strengthening Surveillance of passenger-related operations and other high-interest vessels. The Coast Guard is updating new passenger surveillance and security measures at air and sea port terminals. Designated areas are identified for specific type of vessels birthing at U.S seaports. These vessels are randomly escorted and boarded for security precautions and safe entrances into ports.

Laying the Groundwork for more Comprehensive Security Planning. The Coast Guard is conducting a comprehensive port study through an independent agency to assess the vulnerabilities of more than 50 seaports throughout the U.S. This detail assessment will commence over a three year period.

Driving Maritime Security Worldwide. Planning and coordination with the Maritime International Organizations are on-going. The Coast Guard is seeking ways to develop and expand seaport security worldwide. Actions to expedite advance technology in maritime ship identifications and security plans for port facilities were initially approved in 2002 and now underway. The plan is being managed by the Coast Guard to present to the entire organization.

Inspecting containers and other cargoes. U.S. Customs have begun inspecting vehicles and cargo entering U.S. seaports through the use of new mobile technology imaging and scanning devices. Customs have also

developed a computer-base model to better assist in identifying containers for inspections. This new system of technology will expand Custom intelligence capability to determine the container content and whether it requires additional inspections. This program was implemented in 2002.

Prescreening cargo. U.S. Customs has entered into an agreement with several international countries such as Canada, France, Belgium and other foreign countries to increase its security awareness. The agreement requires that all containers bound for the U.S. must be prescreened prior to their departure port.

Working with the global trade community. U.S. trade agreements are being established in efforts to protect against acts of terrorism on U.S. borders and international commerce. The advantage to this agreement is, international organizations that enter into this agreement will have their cargo expedited through U.S. entry ports.

The Immigration and Naturalization Service (INS) has also mounted several initiatives to improve its endeavors to enhance border security and eliminate access of illegal aliens attempting to gain access into the United States.²⁹ Since September of 2001, several legislative actions involving INS were imposed on the Office of the U.S. Attorney General and the Secretary of State, these actions include: The 2001 USA Patriot Act stipulated additional requirements for the development of new and improved border security awareness systems that had corrupt-resistant credentials. This system automates the process of personnel identification through the use of biometric technology retinal screening and fingerprint recognition software.³⁰ The 2002 Immigration and Naturalization Service Data Management Improvement Act required security awareness systems and programs be implemented at airports, seaports, and land crossing sites with the largest amount of aliens entering and exiting the U.S., starting in 2003.³¹ INS's continues to develop strategies and systems that identify illegal aliens entering and departing the homeland which may pose a security threat.³²

Additionally, legislation is being presented that requires biometric records to be integrated into the new entry and exit system.³³

Responsibilities at the State and Local Levels

The federal plan is not a national plan, because a national plan goes well beyond the federal government. Homeland security is a shared responsibility among a diverse set of federal, state, local, and non-governmental entities. It is important for civilians and homeland security planners to understand the current level of preparedness needed at non-federal levels in order to assist state and local governments to plan for, coordinate plans, and respond to threats or acts of terrorism. Although no city is fully prepared for a terrorist attack, many U.S. cities have response plans in place. The General Accountability Office (GAO) reports that over 600 local and state Hazardous Material (HAZMAT) teams have been identified to serve as first responders to events involving hazardous cargo.³⁴ In fact, since 9/11 most regional, state, and local organizations have taken measures to improve their maritime security readiness and responsiveness through better planning, training, and exercises.

Challenges and Initiatives being Addressed

Diminishing port security threats and eliminating vulnerabilities is a long-term effort. More than just improving the immediate national response capabilities, the U.S. political resolve and the processes to sustain and institutionalize nation-wide threat reduction and response capabilities at all levels of government is needed. Funding for port security has increased since 9/11. The Federal government has invested more than \$17 billion for port security. Funding is allocated toward supporting the Coast Guard's missions of port security operations, personnel deployment and equipment readiness

overseas, and developmental research for science and technology. Federal grants were additionally awarded to states and private agencies to assist with port facility improvements.³⁵

Achieving U.S. seaport security requires several joint endeavors. As this analysis has shown, securing the U.S. seaports is not a single integrated mission, but a multifaceted set of assorted missions and functions that must be performed jointly by federal, state, local, and a host of other organizations. DHS has expanded its area borders outward so that ports can identify, interdict, and prevent suspicious cargo from directly threaten our country. DHS requires information and intelligence on every single U.S. bound shipping container before it has been loaded onto a foreign ship. CBP officers are “stationed at 58 overseas ports [that account] for 86 percent of the container traffic that comes to the United States. [DHS has] deployed equipment overseas to scan cargo for radiation before it leaves for our country [and has] proposed new regulations to collect more commercial data from the private sector [to] better track international shipments.”³⁶ DHS is currently developing a comprehensive national strategy that will provide a roadmap for joint, integrated action and for realizing the leverage and synergy that is attainable only through joint operations with international, federal, state, and local participants to include the DOD. This master plan plays a critical role in securing the homeland.

U.S. port security requires joint operational concepts. Despite the large number of federal homeland security strategies disseminated in the wake of 9/11, none provide “clear joint or interagency operating concepts. These policy documents provide general guidance regarding the goals of homeland security and the need to share information

and coordinate, but none recommend the formulation of a joint operations concept.”³⁷

This is an incredible strategic gap, considering the widespread “perception that DHS was created in order to ‘consolidate’ federal homeland security efforts.”³⁸

Port security efforts must be adequately resourced. This means more than just providing funding to agencies at the federal and state levels, such as funding the Coast Guard for port security operations and deployments, or hardening physical assets and infrastructures, or adding personnel and improving equipment. Port security requires a paradigm shift. The immediate national response must focus on creating U.S. concepts for joint or interagency operations and on processes in place to sustain and maintain nation-wide capabilities for port security. The need to ensure and enable a safer America and its seaports is evident from the studies and commissions conducted after 9/11. There are many common-sense measures being implemented to protect our ports. New restrictions and regulations are implemented for seaports and maritime facilities throughout the nation. Companies are required to file security plans with the Coast Guard that identifies its vulnerabilities along with a feasible, suitable, and acceptable plan to mitigate risk. Nearly 80,000 maritime employees are enrolled into the Transportation Identification Credential (TIC) program by the Coast Guard. There are considerable improvements in container management at the ports; virtually all containers are scanned for radiation upon their arrival to prevent the entry of potential weapons of mass destruction. Prior to 9/11, no cargo was scanned.”³⁹ Securing the homeland is not a single integrated mission but a complex set of diverse missions and functions performed jointly by a number of organizations facing potential threats which could occur in locations nationwide. The success of homeland security hinges on

cooperation and coordination of multiple independent elements acting at different levels. DHS and its security partners face the challenge of devising a comprehensive national strategy that is a roadmap for joint, integrated action and for realizing the leverage and synergy that is attainable only through joint operations of federal, state and local parties. DOD is a significant participant in this endeavor; its enormous capabilities can be skillfully incorporated in the overall security strategy.

However, all responsible parties should commit to more joint training and education. DHS, DOD, and other civilian agencies must improve their joint effort to share information and intelligence. All parties must learn how agencies at the local, state, and federal level fit within the wide range of DHS activities and the broad framework of homeland security strategy. Joint education strategies among agencies pre-9/11 focused predominately on technical matters and rarely involved studying other agencies procedures or participating in joint exercises. Since 9/11, the education and training for port and maritime security have evolved into a Six State Maritime Academies Port and Maritime Security Working Group (PMSWG). This Group's education and training programs are designed to support and strengthen port and maritime security at all levels and entities. Port Maritime Academies are currently established in California, Great Lakes, Maine, Massachusetts, New York, and Texas. Each Academy focuses on specific task in port and maritime security education, training, and assessment.

DHS has developed a comprehensive port security strategy with joint exercises along with DOD and other local, state, and federal agencies. This strategy focuses on the following three areas: prevention, protection, and response and recovery. First, plan

carefully to prevent attacks before they occur. A variety of specific capabilities enhance prevention to detect impending attacks and deter them; both military and civilian agencies play a major role in preventing attacks on our ports. The key to prevention is maritime intelligence. Civilian intelligence agencies, along with DOD, are currently challenged with issues of sharing and integrating intelligence from other domestic and foreign sources. DHS, along with the DOD and civil agencies, must jointly develop new command and control intelligence architectures, linkages, and dissemination processes, while resolving civil liberties and national security concerns. This joint effort must meet the needs of state and local authorities' need for vital and critical intelligence.

Second, Port security protection covers a wide spectrum of requirements to improve the nation's ability to safeguard and defend itself, once attacks occur. The complexity of potential threats and the countermeasures to preempt these threats requires participation from numerous groups at different levels across the nation that can conduct joint protection operations. Building effective joint protection of the ports is indeed a challenge.

Third, DHS is challenged to determine, define, develop, and train the appropriate civilian agencies at the local, state, and federal levels to respond effectively to attacks on our ports and to restore port operations in a timely manner. DHS must seek assistance from DOD on respond and recovery issues because of the subject matter expertise they bring to joint planning, doctrine, training and operations.

Above all this is a joint nation-wide mission. What has become evident from this review is that port security and securing the homeland is not a single integrated mission but a complex set of diverse missions and functions that must be performed jointly by a

number of organizations facing potential threats which could occur in locations nationwide. The success of port security within homeland security centers on cooperation and coordination of multiple independent elements acting at different levels. The Department of Homeland Security faces the challenge of formulating a comprehensive national strategy that is a roadmap for joint, integrated actions and understanding the leverage and combined effort that is only attained through joint operations of federal, state and local organizations.

Conclusions

The 9/11 terrorist attacks on the World Trade Center in New York and the Pentagon in Washington, D. C. changed Americans' view of homeland security and of the Nation's ability to prevent, protect and respond if we are attacked again. Americans now have a new consciousness of the nation's vulnerability to terrorism and a sense of urgency concerning homeland security and defense. DHS was created to ensure a secure homeland, but to date DHS has not achieved seamless security at U.S. seaports, but has led initiatives that moves the nation in the right direction.

These inferences are that the mission of homeland security is a long-term commitment. Americans have to anticipate that asymmetric terrorist threats will continue to occur. Securing the homeland from these threats and attacks requires a broad spectrum of capabilities. These cover prevention and deterrence, protection, and response and recovery from attacks and threats.

The mission of port security is primarily civilian in nature. Most of the complex missions of protecting, deterring, and responding to acts of terrorism against civilian

targets on U.S. soil, such as port and border inspections, are legitimate expressions of civil authority in accordance with the U.S. Constitution.

A national plan for port security requires joint actions of federal, state, and local authorities and non-governmental participants. The national focus should focus on enhancing local capabilities because terrorist acts occur at the local level. Above all, port security is a joint nation-wide mission. Success hinges on the joint, integrated actions of multiple, independent, federal, state, and local entities. The Department of Homeland defense is one the key participants.

Success against terrorism on American soil also requires the participation of the military as one of the U.S. instruments of national power. However, DHS is the primary component of homeland security and is responsible for keeping the homeland secure and responding to terrorist attacks.

Ample legal authority exists for the President to use instruments of national power to respond to serious domestic emergencies. To ensure the appropriate and legal actions can be executed during domestic responses, the President and the Congress should publish guidance explaining the constitutional and statutory authorities and their appropriate implementation in specific circumstance.

While many agree that Coast Guard, CBP, and INS programs to address the threat are sound, DHS contends that these programs represent only a framework for building a maritime security regime, and that significant gaps in security remain.”⁴⁰ Our national security and prosperity depends on secure and competitive ports.

Finally, we know that no single federal, state, local or private entity can create and sustain a flawless security system. However, DHS has dramatically brought to the

forefront the importance of protecting our ports. We have built robust layers of security that have made our ports more secure and less vulnerable than they have ever been. DHS, DOD, and our partners in industry have done this without jeopardizing the fundamental reason for establishing and operating ports in the first place; the economical movement of people and commercial goods. America and its allies cannot let their guard down. We must continue to remain vigilant in our actions involving U.S. seaport security.

Endnotes

¹ *The National Strategy for Maritime Security*, (Washington DC: U.S. Department of Homeland Security September 2005), available from http://www.dhs.gov/interweb/assetlibrary/HSPD13_MaritimeSecurityStrategy.pdf; (accessed November 15, 2008).

² U.S. Department of Homeland Security, "Maritime Commerce Security Plan," (October 2005), 2-3, http://www.dhs.gov/dhspublic/interapp/editorial_0608.xml/ (accessed November 15, 2008).

³ Andrew C. Henrikson, "An Interagency Approach to U.S. Port Security", *Strategic Insights*, 4, no.2 (February 2005) <http://www.ccc.nps.navy.mil/si/2005/Feb/henriksonfeb05.asp#author> (accessed November 19, 2008).

⁴ U.S. Government Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful* (Washington, DC: U.S. Government Printing Office, 2002), 11.

⁵ Andrew C. Henrikson, "An Interagency Approach to U.S. Port Security", *Strategic Insights*, 4, no.2 (February 2005) <http://www.ccc.nps.navy.mil/si/2005/Feb/henriksonfeb05.asp#author> (accessed November 19, 2008).

⁶ Ibid

⁷ Ibid

⁸ U.S. Government Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful* 2002, 5

⁹ Ibid 5

¹⁰ Ibid., 2

¹¹ Harold Relyea, *Homeland Security: The Presidential Coordination Office*, (Washington, DC: Congressional Research Service, 2004)

¹² U.S. Government Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful* 2002), 2

¹³ Ibid., 6

¹⁴ Ibid

¹⁵ *Maritime Transportation Security Act of 2001*, Committee Reports for the 107th Congress, Senate Report 107-064,

¹⁶ Ibid.

¹⁷ Niall Ferguson, "2001," *New York Times Magazine*, December 2, 2001, 78.

¹⁸ Ibid.

¹⁹ Ibid.

²⁰ Ibid.

²¹ Jeffery Blake, *Terrorism and the Military's Role in Domestic Crisis Management: Background and Issues for Congress*, Committee Report for Congress, (Washington DC: United States Congress April 19, 2001), p.2.

²² Ibid

²³ U.S. Department of Homeland Security, *The National Strategy for Homeland Security, National Infrastructure Protection Plan, Executive Summary, 2002*. (Washington DC: U. S. Department of Homeland Security) <http://www.dhs.gov/xlibrary/assets/nipp/plan/execsumm.pdf> (accessed December 8 2008)

²⁴ U.S. Government Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, 6

²⁵ Jennifer E Lake, and Blas Nunez-Neto, *Homeland Security Department: FY2007 Appropriations* (Washington, DC: Congressional Research Service), 2006

²⁶ Ibid.

²⁷ Henrikson, "An Interagency Approach to U.S. Port Security"

²⁸ U.S. Government Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, 6-8

²⁹ Ibid., 8-9

³⁰ Ibid

³¹ Ibid., 8

³² Ibid., 9

³³ Ibid.

³⁴ U.S. Government Accounting Office, *Combating Terrorism: Use of National Guard Response Teams is Unclear*, (Washington, DC: U.S. General Accounting Office, June, 1999), 7.

³⁵ Michael Chertoff, "A Fresh Look at Port Security" *U.S. Department of Homeland Security Leadership Journal*, (February 22, 2008).

³⁶ Ibid.

³⁷ Ibid.

³⁸ Henrikson, "An Interagency Approach to U.S. Port Security" p. 8

³⁹ Chertoff, "A Fresh Look at Port Security,"

⁴⁰ The America's Intelligence Wire, "Department Of Homeland Security Faces Challenges" 2005 *Financial Times*, June 26, 2005.